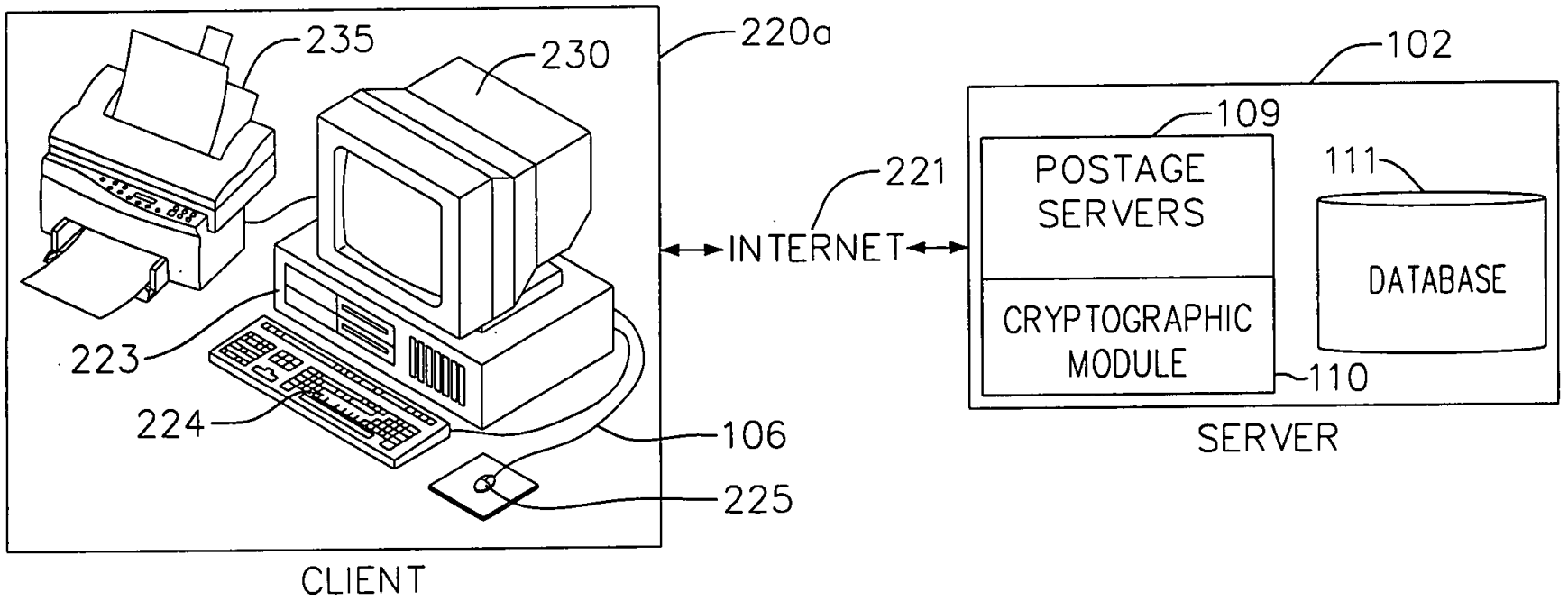
FIG. 1


235
230
220a
102
109
221
POSTAGE SERVERS
111
INTERNET
DATABASE
CRYPTOGRAPHIC MODULE
110
223
224
106
225
CLIENT
SERVER

002TOF 96206960

FIG.2

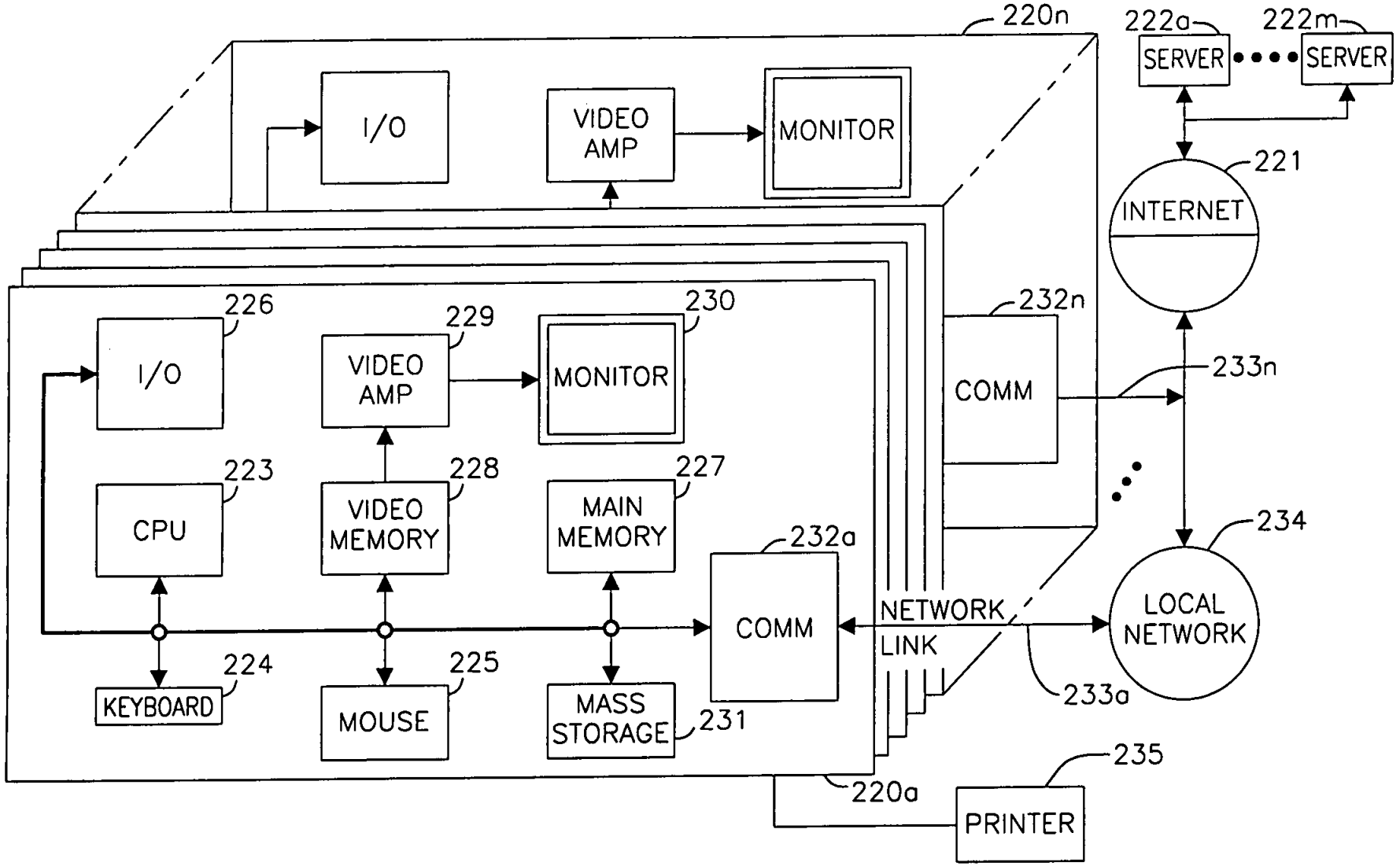


FIG. 3

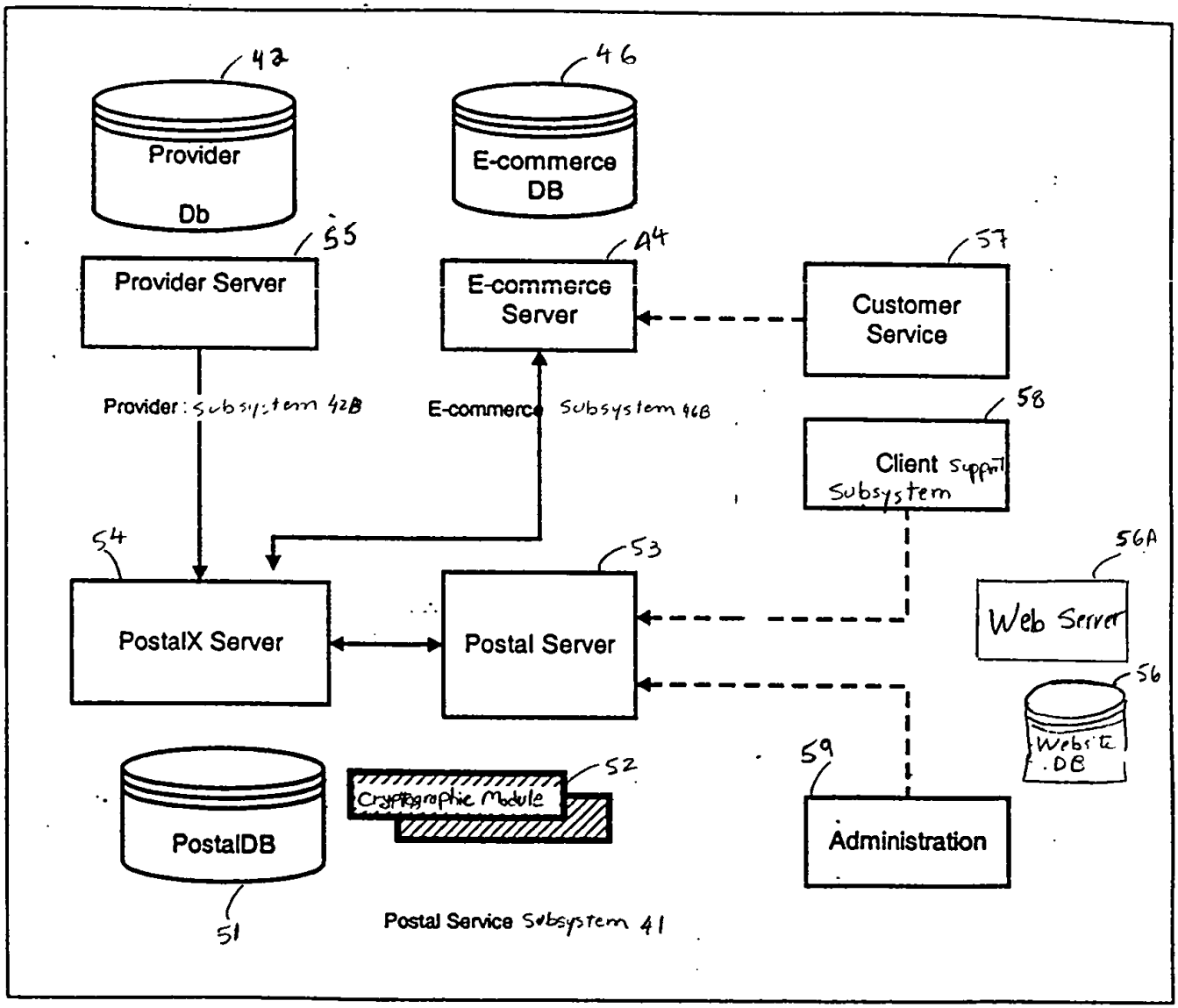
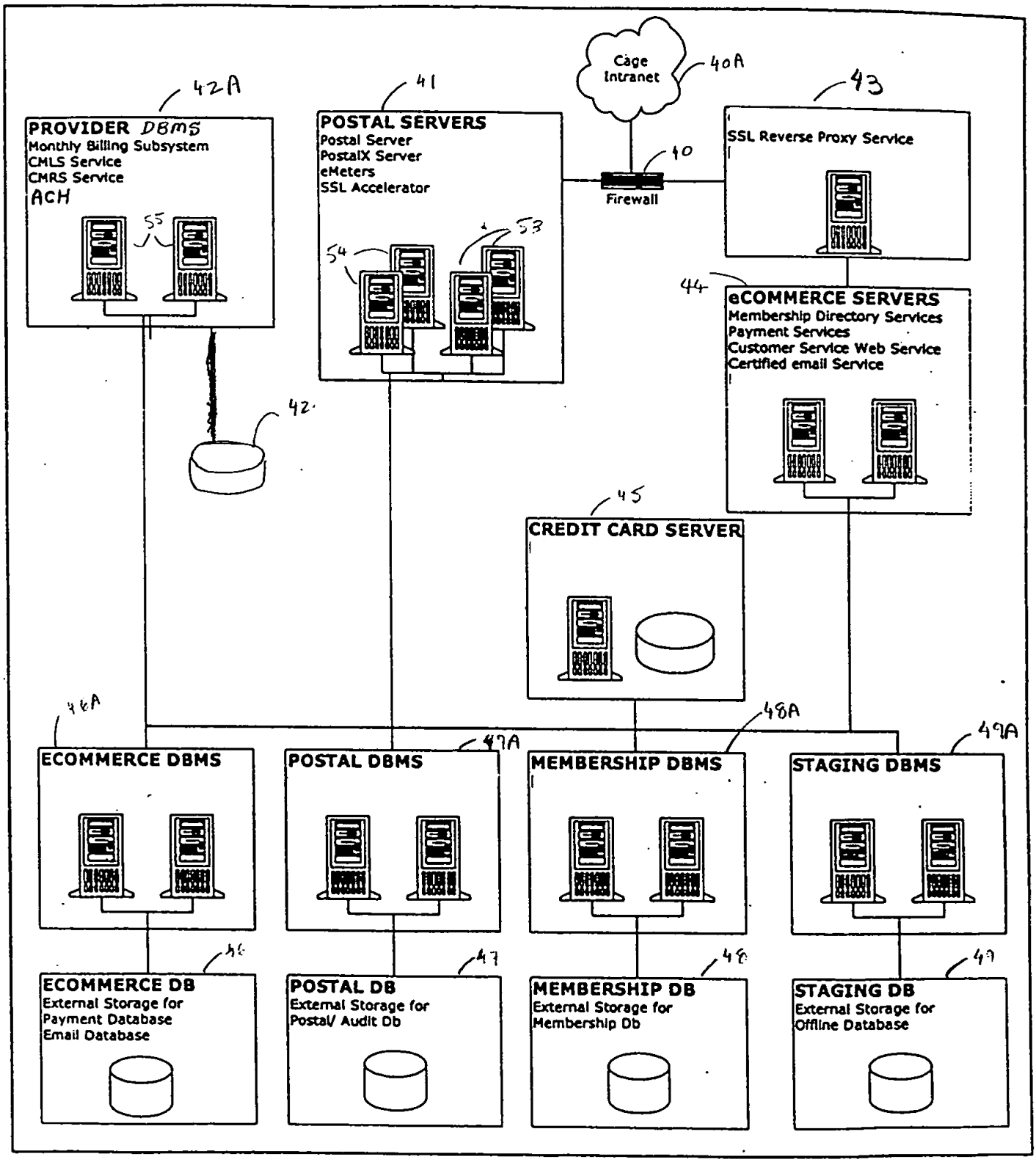

42
Provider
Db
46
E-commerce
DB
55
Provider Server
44
E-commerce
Server
57
Customer
Service
Provider : Subsystem 42B
E-commerce Subsystem 46B
58
Client Support
Subsystem
54
PostalX Server
53
Postal Server
56A
Web Server
56
Website
DB
59
Administration
52
Cryptographic Module
PostalDB
51
Postal Service Subsystem 41

FIG. 4



0074005.960960

FIG. 4A

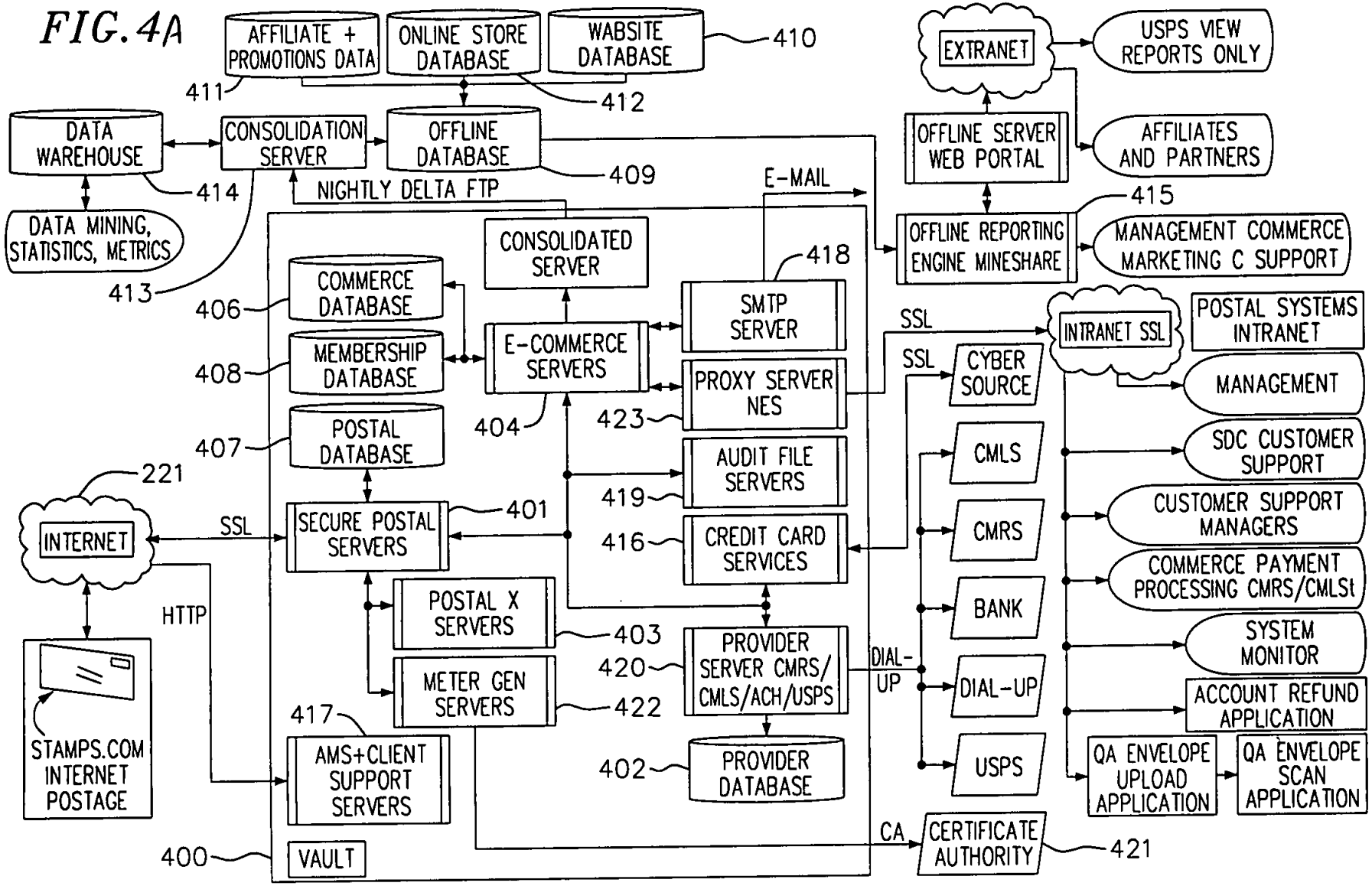
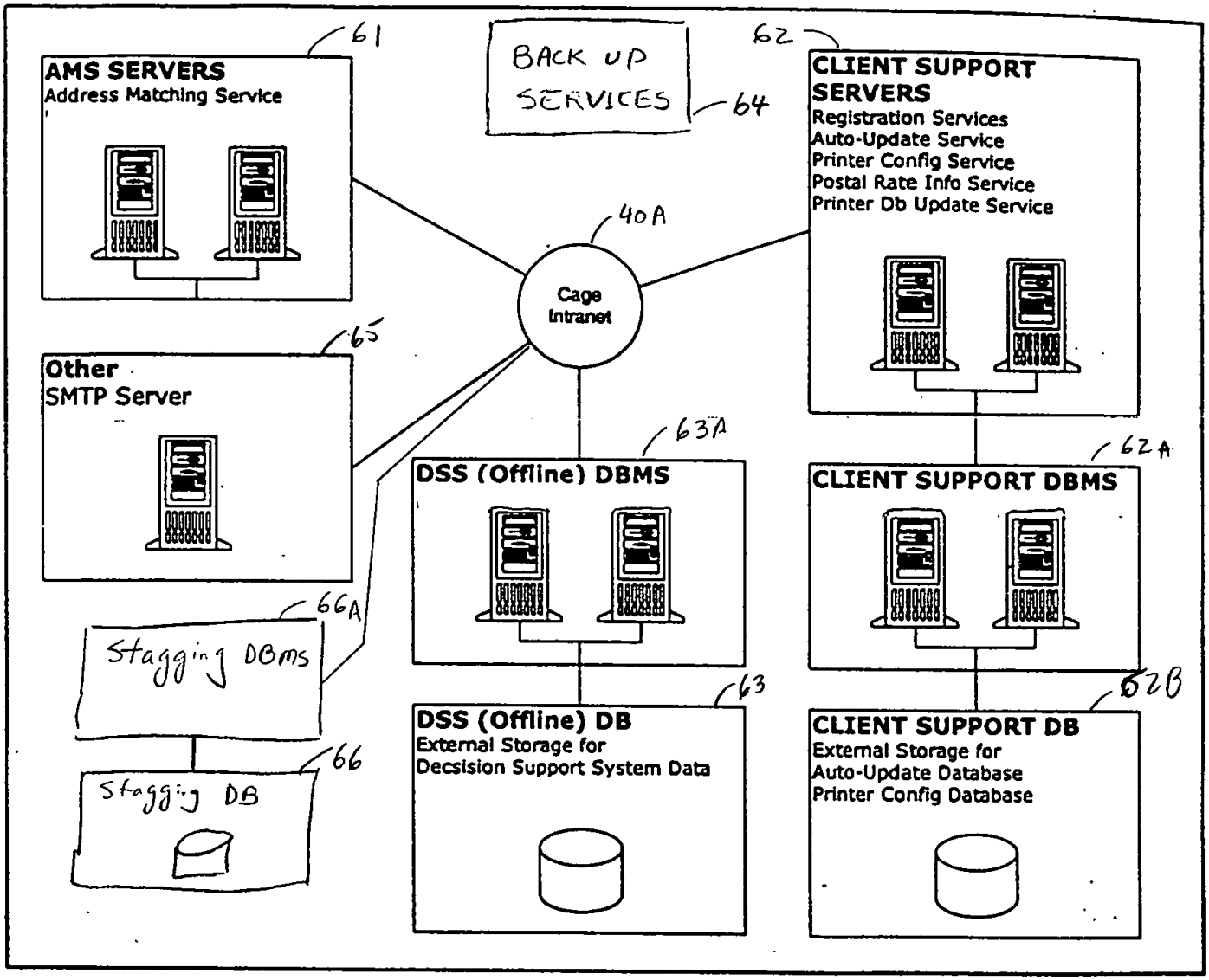

AFFILIATE + PROMOTIONS DATA
ONLINE STORE DATABASE
WABSITE DATABASE
410
411
412
DATA WAREHOUSE
CONSOLIDATION SERVER
OFFLINE DATABASE
409
414
NIGHTLY DELTA FTP
E-MAIL
DATA MINING, STATISTICS, METRICS
413
CONSOLIDATED SERVER
418
COMMERCE DATABASE
406
SMTP SERVER
MEMBERSHIP DATABASE
408
E-COMMERCE SERVERS
PROXY SERVER NES
423
404
POSTAL DATABASE
407
AUDIT FILE SERVERS
419
221
INTERNET
SSL
SECURE POSTAL SERVERS
401
CREDIT CARD SERVICES
416
POSTAL X SERVERS
403
HTTP
PROVIDER SERVER CMRS/ CMLS/ACH/USPS
420
METER GEN SERVERS
422
DIAL-UP
STAMPS.COM INTERNET POSTAGE
417
AMS+CLIENT SUPPORT SERVERS
PROVIDER DATABASE
402
400
VAULT
CA
CERTIFICATE AUTHORITY
421
EXTRANET
USPS VIEW REPORTS ONLY
OFFLINE SERVER WEB PORTAL
AFFILIATES AND PARTNERS
415
OFFLINE REPORTING ENGINE MINESHARE
MANAGEMENT COMMERCE MARKETING C SUPPORT
SSL
INTRANET SSL
POSTAL SYSTEMS INTRANET
SSL
CYBER SOURCE
MANAGEMENT
CMLS
SDC CUSTOMER SUPPORT
CMRS
CUSTOMER SUPPORT MANAGERS
BANK
COMMERCE PAYMENT PROCESSING CMRS/CMLS
SYSTEM MONITOR
DIAL-UP
ACCOUNT REFUND APPLICATION
USPS
QA ENVELOPE UPLOAD APPLICATION
QA ENVELOPE SCAN APPLICATION

FIG. 5



DOCKET: 96/056,050

FIG. 6

002701" 96206960

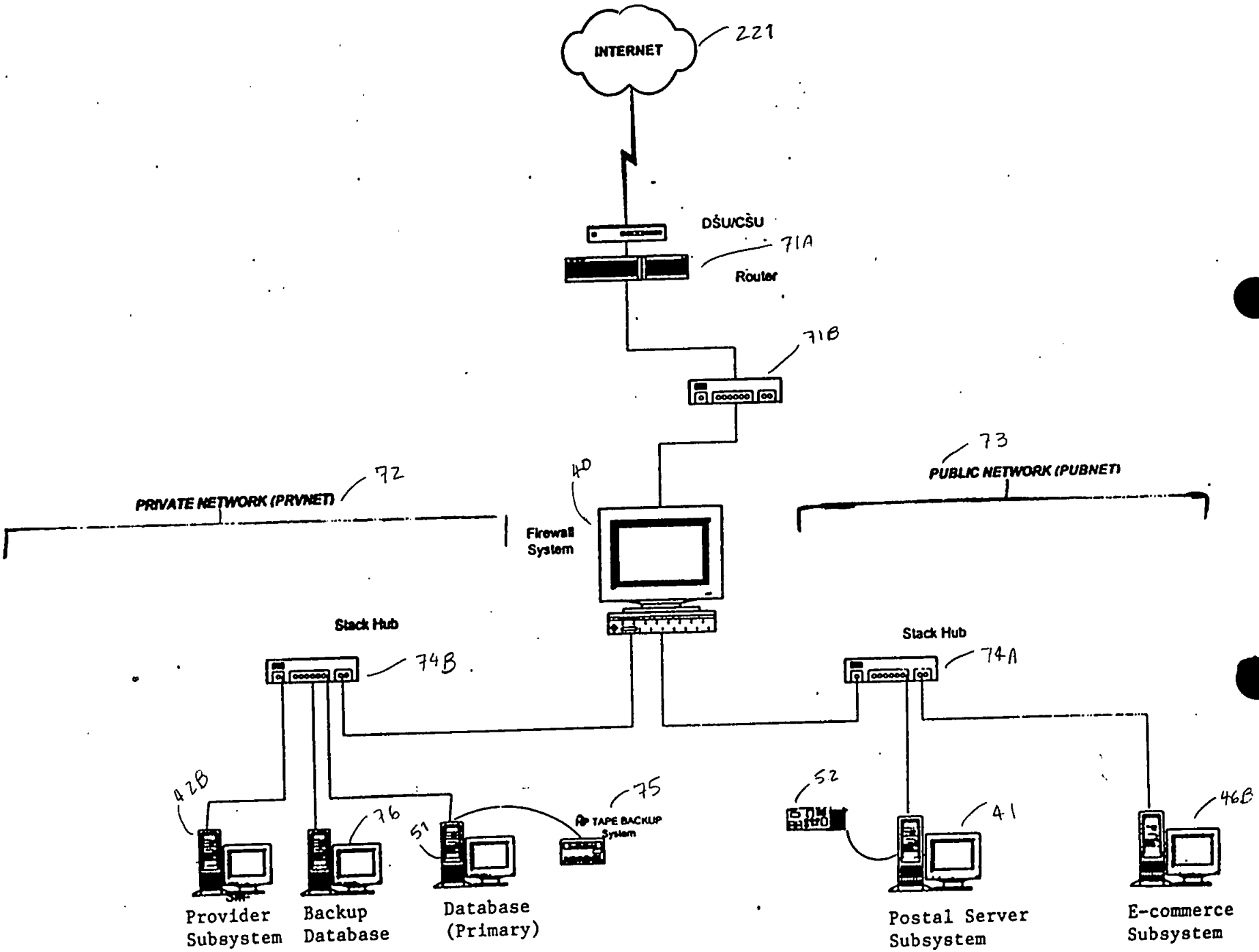
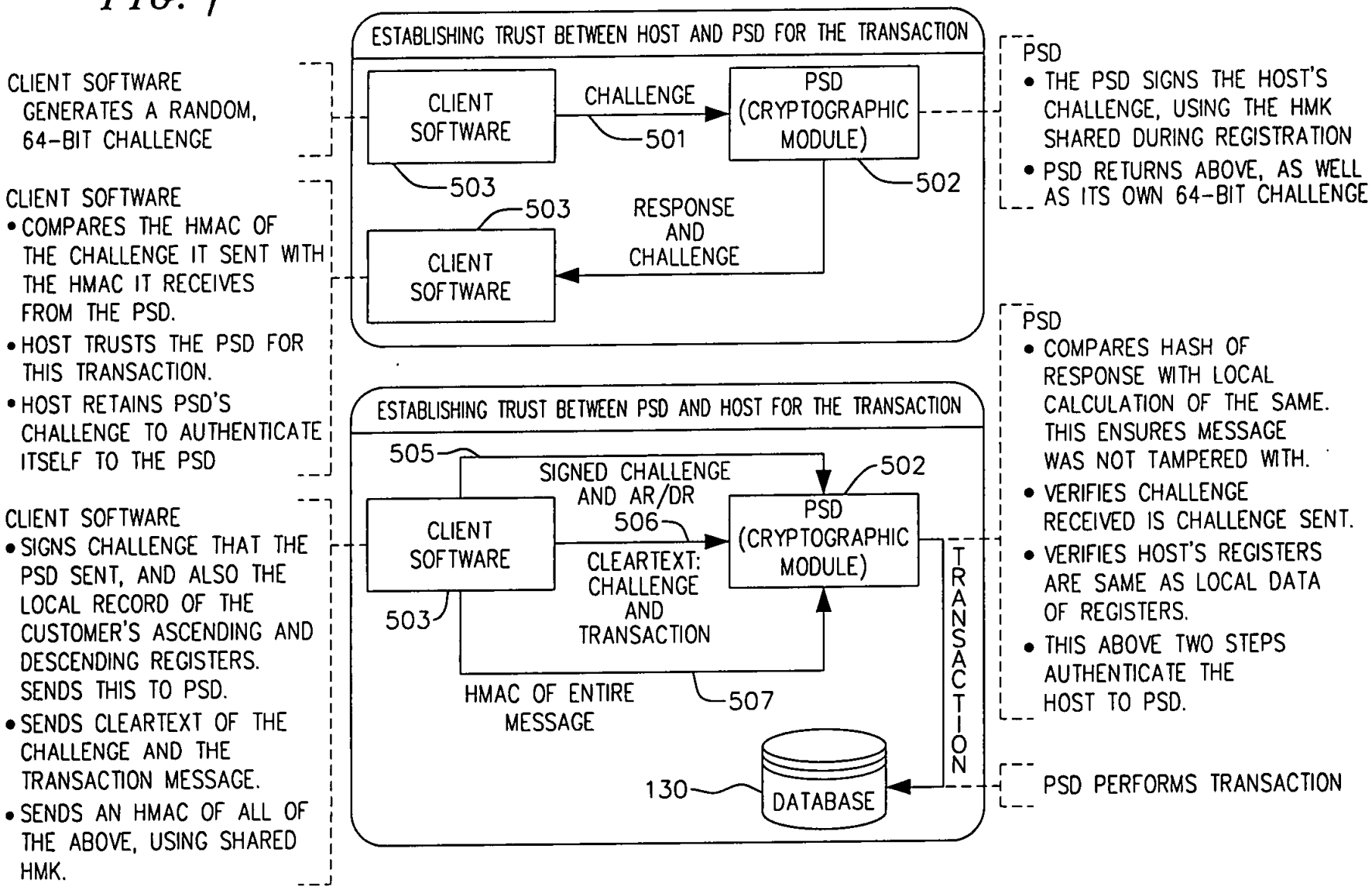


FIG. 7


ESTABLISHING TRUST BETWEEN HOST AND PSD FOR THE TRANSACTION
CLIENT SOFTWARE GENERATES A RANDOM, 64-BIT CHALLENGE
CLIENT SOFTWARE
CHALLENGE
501
PSD (CRYPTOGRAPHIC MODULE)
502
503
503
RESPONSE AND CHALLENGE
CLIENT SOFTWARE
CLIENT SOFTWARE
• COMPARES THE HMAC OF THE CHALLENGE IT SENT WITH THE HMAC IT RECEIVES FROM THE PSD.
• HOST TRUSTS THE PSD FOR THIS TRANSACTION.
• HOST RETAINS PSD'S CHALLENGE TO AUTHENTICATE ITSELF TO THE PSD
PSD
• THE PSD SIGNS THE HOST'S CHALLENGE, USING THE HMK SHARED DURING REGISTRATION
• PSD RETURNS ABOVE, AS WELL AS ITS OWN 64-BIT CHALLENGE
ESTABLISHING TRUST BETWEEN PSD AND HOST FOR THE TRANSACTION
505
SIGNED CHALLENGE AND AR/DR
502
506
CLIENT SOFTWARE
PSD (CRYPTOGRAPHIC MODULE)
CLEARTEXT: CHALLENGE AND TRANSACTION
503
HMAC OF ENTIRE MESSAGE
507
TRANSACTION
130
DATABASE
CLIENT SOFTWARE
• SIGNS CHALLENGE THAT THE PSD SENT, AND ALSO THE LOCAL RECORD OF THE CUSTOMER'S ASCENDING AND DESCENDING REGISTERS. SENDS THIS TO PSD.
• SENDS CLEARTEXT OF THE CHALLENGE AND THE TRANSACTION MESSAGE.
• SENDS AN HMAC OF ALL OF THE ABOVE, USING SHARED HMK.
PSD
• COMPARES HASH OF RESPONSE WITH LOCAL CALCULATION OF THE SAME. THIS ENSURES MESSAGE WAS NOT TAMPERED WITH.
• VERIFIES CHALLENGE RECEIVED IS CHALLENGE SENT.
• VERIFIES HOST'S REGISTERS ARE SAME AS LOCAL DATA OF REGISTERS.
• THIS ABOVE TWO STEPS AUTHENTICATE THE HOST TO PSD.
PSD PERFORMS TRANSACTION